

REMARKS

In the Official Action mailed on **5 December 2005**, the Examiner reviewed claims 1, 4, 7-12, 15, 18-23, 26 and 29-33. Claims 1, 4, 7-12, 15, 18-23, 26, and 29-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dickinson et al (USPN 6,853,988, hereinafter "Dickinson").

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 12, and 23 were rejected as being unpatentable over Dickinson. Applicant respectfully points out that Dickinson teaches authenticating a user and digitally signing a form using the private key of a user (see Dickinson, column 47, lines 31-44). The authentication process involves using authentication data which is **user-specific** (see Dickinson, column 7, lines 13-21). The user-specific authentication data includes a user identification number, one or more biometrics, a series of questions, etc. (see Dickinson, column 7, lines 13-21; and column 18, line 36 to column 19, line 9).

In contrast, the present invention receives **a user identifier and an application identifier** (see page 9, lines 20-21 of the instant application), and looks up a key pair based on **a user identifier and an application identifier** (see page 10, lines 9-14 of the instant application). The present invention then uses the identified private key to sign a form on behalf of the user (see page 10, lines 15-16 of the instant application). This is beneficial because it allows the signature server to sign a document on behalf of a user *only if* the user is allowed to sign for a given application. Hence, even if the user has a valid key pair for other applications, the signature server will not sign on behalf of the user unless the user is authorized to sign for the given application.

There is nothing within Dickinson, either explicit or implicit, which suggests receiving a user identifier and an application identifier at a signature

server, and looking up a private key for the user based on the user identifier and the application identifier.

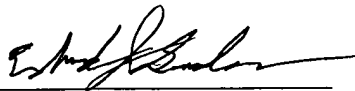
Accordingly, Applicant has amended independent claims 1, 12, and 23 to clarify that the present invention (1) receives the message from the user at the signature server, the message including an item to be signed on behalf of the user by the signature server, *a user identifier which identifies the user, and an application identifier which identifies the application being used*; and (2) looks up a private key for the user at the signature server *based on the user identifier and the application identifier*. These amendments find support in on page 9, lines 20-21, and page 10, lines 9-14 of the instant application

Hence, Applicant respectfully submits that independent claims 1, 12, and 23 as presently amended are in condition for allowance. Applicant also submits that claims 4 and 7-11, which depend upon claim 1, claims 15 and 18-22, which depend upon claim 12, and claims 26 and 29-33, which depend upon claim 23, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 
Edward J. Grundler
Registration No. 47,615

Date: 6 March 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
edward@parklegal.com